REMARKS

This application has been carefully reviewed in light of the Office Action dated November 1, 2007. Claims 1, 3 to 8, 10, 13 and 14 remain in the application, with Claims 2, 9, 11, 12 and 15 having been canceled herein. Claims 1, 13 and 14 are independent. Reconsideration and further examination are respectfully requested.

Claims 1 to 15 have been rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 7,020,456 (Smeets) in view of U.S. Patent No. 6,526,506 (Lewis). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention concerns establishing two different types of communication links between an access point device and a client terminal. In the present invention, a first cipher key and a network identifier are displayed on a display unit of the access point device, the key and identifier being for establishing a first wireless link between the access point device and the client without the need for an authentication process. By inputting the displayed key and identifier, the first wireless link, without the authentication process, is established. Once the first link is established, the client terminal is displayed on the display unit of the access point device. A determination is then made, based on a user's operation, whether the client terminal is authorized to participate in the network with a second wireless communication that does require authentication. If so, then authentication data is sent from the access point device to the client terminal through the first communication link, the first link is discarded, and the second wireless communication link is established through the authentication process, where the second link has the same network identifier as the first link.

With specific reference to the claims, Claim 1 is directed to a network configuration method of configuring a wireless network, comprising an access point device receiving a network configuration request for configuring a new wireless network comprising the access point device and at least one client terminal, a first display step of displaying a first cipher key and a network identifier on a display unit of the access point device, the first cipher key and the network identifier being used for establishing a first wireless communication link through a first encrypted communication that does not require an authentication process, a first link establishing step of establishing, between the access point device and a client terminal, the first wireless communication link by inputting the first cipher key and the network identifier into the client terminal, a second display step of displaying the client terminal on the display unit of the access point device, the first wireless communication link having been established between the client terminal and the access point device in the first link establishing step, a determination step of determining whether the client terminal is to be authorized to participate in the network which is configured with a second wireless communication link through a second encrypted communication that requires the authentication process, where the client terminal is determined on the basis of a user operation from among client terminals which are displayed in the second display step, a sending step of, if the determination step determines that the client terminal is authorized to be configured in the network with the access point device, the access point device sending authentication data from the access point device to the client terminal in a state where the first wireless communication link through the first encrypted communication is established, a link discarding step of discarding the first wireless communication link through the first encrypted

communication between the access point device and the client terminal in response to the sending of the authentication data to the client terminal by the access point device at the sending step, and a second link establishing step of establishing, between the access point device and the client terminal, the second wireless communication link through the second encrypted communication that requires the authentication process using the authentication data sent to the client terminal after discarding the first communication link at the link discarding step, the second wireless communication link having the same network identifier as that of the first wireless communication link.

Claim 13 is a system and Claim 14 is an access point device claim, each of which include features substantially corresponding to Claim 1.

The applied art, alone or in any permissible combination, is not seen to disclose or to suggest the features of Claims 1, 13 and 14, and in particular, the applied art is not seen to disclose or to suggest at least the features of using a first cipher key and a network identifier displayed on a display unit of an access point device for establishing a first wireless communication link between the access point and a client terminal through a first encrypted communication that does not require an authentication process, displaying the client terminal on the display unit of the access point device when the first wireless communication link has been established, determining whether the client terminal is to be authorized to participate in the network which is configured with a second wireless communication link through a second encrypted communication that requires the authentication process, where the client terminal is determined on the basis of a user operation from among client terminals which are displayed on the display unit, if the client terminal is authorized to be configured in the network with the access point device, the

access point device sending authentication data from the access point device to the client terminal in a state where the first wireless communication link through the first encrypted communication is established, discarding the first wireless communication link in response to the sending of the authentication data to the client terminal, and establishing, between the access point device and the client terminal, the second wireless communication link through the second encrypted communication that requires the authentication process using the authentication data sent to the client terminal after discarding the first communication link at the link discarding step, the second wireless communication link having the same network identifier as that of the first wireless communication link.

Smeets is seen to disclose that a first communication link between a user device and a first service device is established, an access key code is generated and a data item indicating the access key code is stored in the user device. The access key code is then made available to a second service device, a second communication link is established between the user device and the second service device, and the access key code is used to mutually authenticate the user device and the second service device. Thus, in Smeets, the two communication links that are established are between three different devices, whereas, in the present invention, two links are established between two devices. That is, in Smeets, the first link is between devices A and B, while the second link is between devices A and C, with the second link between A and C being authenticated. The invention established a first link between A and B without authentication, provides authentication data from device A to B, discards the first link between A and B, establishes a second link between A and B using the authentication data. Smeets, therefore, is clearly not seen to disclose or to suggest at least the features of using a first cipher key and a network identifier displayed

on a display unit of an access point device for establishing a first wireless communication link between the access point and a client terminal through a first encrypted communication that does not require an authentication process, displaying the client terminal on the display unit of the access point device when the first wireless communication link has been established, determining whether the client terminal is to be authorized to participate in the network which is configured with a second wireless communication link through a second encrypted communication that requires the authentication process, where the client terminal is determined on the basis of a user operation from among client terminals which are displayed on the display unit, if the client terminal is authorized to be configured in the network with the access point device, the access point device sending authentication data from the access point device to the client terminal in a state where the first wireless communication link through the first encrypted communication is established, discarding the first wireless communication link in response to the sending of the authentication data to the client terminal, and establishing, between the access point device and the client terminal, the second wireless communication link through the second encrypted communication that requires the authentication process using the authentication data sent to the client terminal after discarding the first communication link at the link discarding step, the second wireless communication link having the same network identifier as that of the first wireless communication link.

Lewis is not seen to disclose anything that, when combined with Smeets, would have resulted in the present invention. In this regard, Lewis is merely seen to disclose the use of a multilevel encryption scheme in a wireless network. However, Lewis is not seen to teach anything that, when combined with Smeets, would have resulted in the

features of using a first cipher key and a network identifier displayed on a display unit of an access point device for establishing a first wireless communication link between the access point and a client terminal through a first encrypted communication that does not require an authentication process, displaying the client terminal on the display unit of the access point device when the first wireless communication link has been established, determining whether the client terminal is to be authorized to participate in the network which is configured with a second wireless communication link through a second encrypted communication that requires the authentication process, where the client terminal is determined on the basis of a user operation from among client terminals which are displayed on the display unit, if the client terminal is authorized to be configured in the network with the access point device, the access point device sending authentication data from the access point device to the client terminal in a state where the first wireless communication link through the first encrypted communication is established, discarding the first wireless communication link in response to the sending of the authentication data to the client terminal, and establishing, between the access point device and the client terminal, the second wireless communication link through the second encrypted communication that requires the authentication process using the authentication data sent to the client terminal after discarding the first communication link at the link discarding step, the second wireless communication link having the same network identifier as that of the first wireless communication link.

In view of the foregoing deficiencies of the applied art, amended independent Claims 1, 14 and 15, as well as the claims dependent therefrom, are believed to be allowable.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

/Edward Kmett/

Edward A. Kmett
Attorney for Applicant
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

FCHS_WS 1944568v1